

Application Serial No. 10/594,106
Reply to office action of December 27, 2007

PATENT
Docket: CU-5118

Amendments To The Abstract

Marked-up Version

The following marked-up version of the amended Abstract is attached hereto to aid the examiner in identifying the changes; please note that "Figure 2" has already been deleted in the preliminary amendment filed on April 10, 2007:

INVENTION PATENT

**DEVICE AND METHOD FOR THE DETECTION AND PREVENTION OF INTRUSION
INTO A COMPUTER NETWORK**

NETASQ

3 RUE ARCHIMEDE

59650 VILLENEUVE D'ASCQ

ABSTRACT

A device and a method for the detection and prevention of intrusion into a computer network by detecting and blocking the intrusions before penetration of the network. The method includes a stage for detecting the connections at the central point and before each branch of the network, and a stage for selective filtering of these connections. This selective filtering of the connections includes a stage for automatic recognition of the accessing protocol, independently of the communication port used by the protocol.

Application Serial No. 10/594,106
Reply to office action of December 27, 2007

PATENT
Docket: CU-5118

REMARKS/ARGUMENTS

Reconsideration is respectfully requested.

Claims 1-12 are pending before this amendment. By the present amendment; claims 1-7 are amended. No new matter has been added.

In the office action (page 2), the arrangement of the specification stands objected to. The applicants respectfully directs the examiner's attention to the preliminary amendment filed on April 10, 2007, in which the applicants amended the specification to include the section headings: 'BACKGROUND OF THE INVENTION', BRIEF DESCRIPTION OF THE DRAWING FIGURES', AND DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS'. The applicants note that the arrangement of application described by the examiner is a preference and not a requirement (see MPEP 608.01(a) and 37 C.F.R 1.71, 1.77(a-c)). Further, the statement "if no text follows the section heading, the phrase 'Not Applicable' should follow the section heading" is a suggestion and certainly isn't required by 37 C.F.R. 1.71 or C.F.R. 1.77(b). Finally please note that MPEP 601.1 states the requirements of a complete application. The applicants respectfully submit that these requirements have been met. If the applicants are misinterpreting the examiner's objection, please let us know. Otherwise, withdrawal of the objection is respectfully requested.

In the office action (page 2), the abstract stands objected to for containing informalities. In response, the Abstract amended to incorporate the examiner suggestions is attached hereto on a separate page. Please note the abstract was

Application Serial No. 10/594,106
Reply to office action of December 27, 2007

PATENT
Docket: CU-5118

amended previously in the preliminary amendment filed April 10, 2007. Withdrawal of the objection is respectfully requested

In the office action (page 2), the claims stand objected to for containing informalities. In response, the applicants have amended the claims in accordance with the examiner's suggestions to remove any informalities. Withdrawal of the objection is respectfully requested.

In the office action (page 3), claims 1-12 stand rejected under 35 U.S.C. § 102(a) as being anticipated by "NETASQ IPS-Firewalls. ASQ: Real-Time Intrusion Prevention" (AUTHOR UNKNOWN; PUBLISHED: 2003) hereinafter referred to as ASQ V.2.

Also, In the office action (page 7), claims 1-12 stand rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 7,174,566 (YADAV). The "et al." suffix is omitted in a reference name.

The applicants respectfully disagree.

The applicants respectfully submit that the invention as claimed in claims 1 to 12 is neither anticipated by ASQ V.2 nor by YADAV.

The present invention relates to a device (claim 6 and dependant claims) and a method (claim 1 and dependant claims) for the detection and prevention of intrusions into a computer network, which allows for the prevention of such intrusions by detecting them before penetration of the network.

As for claim 1:

Application Serial No. 10/594,106
Reply to office action of December 27, 2007

PATENT
Docket: CU-5118

The method of the invention filters the connections, at the central point and before each branch of the network, through a step, amongst other steps, where the accessing protocol is automatically recognized, independently of the communication port used by this protocol.

Besides, after automatic recognition of this protocol, the conformity of this protocol is verified, in order to deliver a dynamic authorization or rejection for each communication, depending on the conformity or non-conformity of this communication with the protocol.

The protocol analysis is performed from the lowest protocol to the highest protocol in the hierarchy, performing so a conformity check in depth, layer by layer, on each part of the analyzed data packet.

Moreover, the conformity check detects the information necessary to dynamically open the secondary connections or connections induced, depending on the protocol, by the main connection. These secondary connections are thus correctly attached to the authorization of the main connection.

Indeed, it is necessary that all these secondary or induced connections be attached to the authorization of the main connection, for a higher security level. Only a precise and in depth analysis, layer by layer, of the working of the protocol, which is automatically recognized, allows for a precise determination of whether the communication ports are to be opened or closed.

As for claim 6:

Application Serial No. 10/594,106
Reply to office action of December 27, 2007

PATENT
Docket: CU-5118

The device of the invention comprises a resource for preventing intrusions, allowing detection of the connections before each branch of the network, through a resource for selectively filtering the connections by automatic recognition of the accessing protocol, independently of the communication port used by the protocol.

The resource for selectively filtering comprises at least an autonomous analysis module for the analysis of at least one given protocol, which allows the automatic recognition of the protocol, and the verification of the conformity of the communications with this protocol. This autonomous module delivers a dynamic authorization or rejection for each connection, whether this communication is a result from a normal or abnormal working of the protocol. This module is able to transmit a part of a data packet to an autonomous module of analysis of a hierarchically higher protocol.

Therefore, such an autonomous analysis module allows, in combination with potential other autonomous analysis modules of the device, a precise and in depth multilayer protocol analysis in order to determine with precision the communication port to be opened or closed.

As explained above, this is fundamental in order that all the secondary connections or connections induced by a main connection, be correctly attached to the main authorization, i.e. the authorization of the main connection.

As for ASQ V.2 and YADAV :

ASQ V.2 discloses in no way all the above characteristics of claims 1 and 6.

In particular, even if ASQ V.2 mentions the principle of multilayer protocol analysis, it does **not** disclose the specific characteristics according to which the

Application Serial No. 10/594,106
Reply to office action of December 27, 2007

PATENT
Docket: CU-5118

conformity check detects the information necessary to open secondary connections or induced connections and attaches these secondary or induced connections dynamically to the authorization of the main connection.

Even more so, ASQ V.2 does not disclose the transmission by an autonomous analysis module of a part of a data packet to another autonomous analysis module of a hierarchically higher protocol.

As to YADAV, YADAV discloses a method and a device for the detection and prevention of intrusions in a computer network, but does not mention in any way a layer by layer protocol analysis with transmission of part of data packet from an autonomous analysis module of an automatically recognized protocol to another autonomous analysis module of a hierarchically higher protocol.

No mention neither can be found in YADAV with respect to attachment of secondary or induced connections to authorization of the main connection.

For at least these reasons, it is respectfully submitted that claims 1 and 6 are not anticipated by ASQ V.2, nor are they by YADAV.

As to dependent claims 2 to 5 and 7 to 12 the applicants respectfully submit that these claims are allowable at least since they depend from claim 1 or claim 6, which are now considered to be in condition for allowance for the reasons above.

For the reasons set forth above, the applicants respectfully submit that claims 1-12 pending in this application are in condition for allowance over the cited references. Accordingly, the applicants respectfully request reconsideration and withdrawal of the outstanding rejections and earnestly solicit an indication of allowable subject matter.

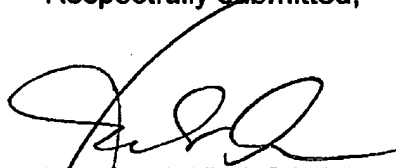
Application Serial No. 10/594,106
Reply to office action of December 27, 2007

PATENT
Docket: CU-5118

This amendment is considered to be responsive to all points raised in the office action. Should the examiner have any remaining questions or concerns, the examiner is encouraged to contact the undersigned attorney by telephone to expeditiously resolve such concerns.

Respectfully submitted,

Dated: July 9, 2008



W. William Park, Reg. No. 55,523
Ladas & Parry LLP
224 South Michigan Avenue
Chicago, Illinois 60604
(312) 427-1300